Fehlerbehebung bei IGMP für NLB-Bereitstellungen auf Catalyst Switches der Serie 9000

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie sich die IGMP-Funktion auf Catalyst Switches der Serie 9000 in einer Microsoft Network Load Balancer (NLB)-Bereitstellung verhält.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Microsoft NLB-Betriebsmodi
- IGMP-Multicast

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Catalyst 9200
- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

NLB ist eine Cluster-Technologie, die in allen Windows 2000 Server- und Windows 2003 Server-Systemen verfügbar ist. Es stellt eine einzige virtuelle IP-Adresse für alle Clients als Ziel-IP-Adresse für das gesamte Cluster bereit.

NLB kann verwendet werden, um Client-Anforderungen auf eine Reihe von Servern zu verteilen. Um sicherzustellen, dass die Clients ein akzeptables Leistungsniveau aufweisen, bietet NLB die Möglichkeit, zusätzliche Server hinzuzufügen, um zustandslose Anwendungen (z. B. IIS-basierte Webserver) zu skalieren, wenn die Client-Last ansteigt. Darüber hinaus werden Ausfallzeiten aufgrund von Serverfehlern reduziert.

Sie können den NLB so konfigurieren, dass er in einem der folgenden drei Modi funktioniert:

- Unicast-Modus
- Multicast-Modus
- Internet Group Management Protocol (IGMP)-Modus

> **Tipp:** Die Bereitstellungen im Unicast- und Multicast-Modus verfügen über die gleiche Konfiguration und Verifizierung, die im Dokument "Catalyst Switches for Microsoft Network Load Balancing Configuration Example" beschrieben ist.

Dieses Dokument behandelt den IGMP-Modus (Internet Group Management Protocol).

Best Practices

Catalyst Switches der Serie 9000 durchsuchen die Layer-3-Header von IGMP-Paketen, um die Snooping-Tabelle zu füllen. Da NLB auf dem Switch mithilfe einer statischen Multicast-MAC-Adresse konfiguriert werden muss, wird die IGMP-Snooping-Tabelle nicht aufgefüllt, und das Ziel-VLAN wird geflutet. Mit anderen Worten: IGMP-Snooping in Catalyst 9000 enthält nicht automatisch die Multicast-Flut, wenn sich der NLB-Server im IGMP-Modus befindet (die Weiterleitung in Catalyst 9000 basiert auf Multicast-IP und nicht auf Multicast-MAC-Adressen).

> **Hinweis**: Auf dem Catalyst 9000 werden alle drei NLB-Modi geflutet. Flooding tritt im Benutzer-VLAN nicht auf, da das Ziel der Pakete ihr Standard-Gateway sein muss. Erst nach dem Umschreiben des Headers in das Ziel-VLAN tritt die Überflutung auf.

Daher sollten Sie diese Best Practices für erfolgreiche Bereitstellungen berücksichtigen:

- Verwenden Sie ein dediziertes VLAN, um die Überflutung auf den NLB-Cluster zu beschränken.
- Verwenden Sie statische MAC-Einträge, um die Ports zu begrenzen, an denen das Flood innerhalb des NLB-VLAN auftritt.

IGMP-Modus

In diesem Modus fällt die virtuelle MAC des NLB-Clusters in den Bereich der Internet Assigned Numbers Authority (IANA) und beginnt bei 0100.5exx.xxxx. Die Fehlermeldung IGMP Snooping Die auf dem Switch konfigurierte Funktion programmiert die virtuelle Multicast-MAC-Adresse des Clusters nicht in der MAC-Adresstabelle. Da diese dynamische Programmierung fehlt, wird der vom Switch empfangene Multicast-Verkehr vom NLB-Cluster an alle Ports desselben VLAN geleitet. Cisco Bug-ID CSCvw18989.

Für Topologien, in denen sich die NLB-Server in einem anderen VLAN als die Benutzer befinden, ist die virtuelle IP-Adresse des Clusters, da sie eine Multicast-MAC-Adresse verwendet, außerhalb des lokalen Subnetzes nicht erreichbar. Um dieses Problem zu beheben, müssen Sie auf jedem Gerät mit einer Layer-3-Schnittstelle im Cluster-VLAN einen statischen ARP-Eintrag konfigurieren.

Die IGMP-Snooping-Funktion der Catalyst Switches der Serie 9000 verwendet die Multicast-MAC-Adresse nicht für die Weiterleitung. Sie verwenden die Multicast-IP-Adresse. Aus diesem Grund ist sie nicht in der

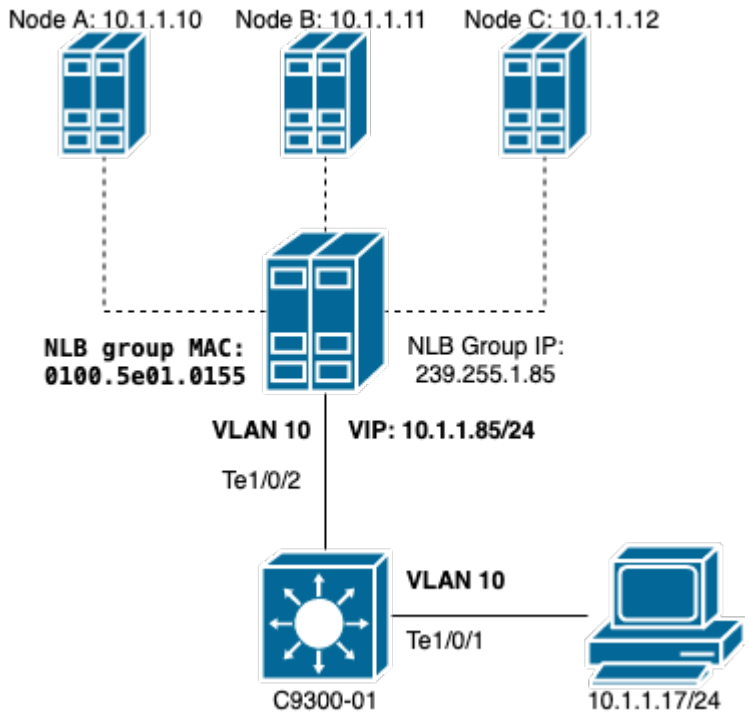
Lage, die Multicast-MAC-Adresse in der MAC-Tabelle automatisch zu programmieren, wie dies bei anderen älteren Plattformen (z. B. der Catalyst Serie 6000) der Fall ist. Alle neuen Plattformen verwenden die Multicast IP Address Forwarding-Methode, um das Problem der sich überschneidenden Adressen auf Legacy-Switches zu vermeiden.

> **Hinweis**: Eine Ethernet-Multicast-MAC-Adresse überschneidet sich teilweise. Dieselbe MAC-Adresse ist 32 unterschiedlichen Multicast-Gruppen zugewiesen. Wenn ein Benutzer eines Ethernet-Segments die Multicast-Gruppe 225.1.1.1 und ein anderer Benutzer die Gruppe 230.1.1.1 abonniert, erhalten beide Benutzer beide Multicast-Streams (MAC-Adresse ist dieselbe 01-00-5e-01-01-01). Bei der Entwicklung von Multicast-Netzwerken in LAN-Segmenten muss diese Überlappung genau beobachtet und entwickelt werden, um das Problem zu vermeiden.

Konfigurieren

Quelle und Ziel im selben VLAN

Netzwerkdiagramm



In diesem Abschnitt wird beschrieben, wie Sie den NLB konfigurieren, wenn sich der Cluster und die Benutzer im gleichen VLAN befinden.

1. Überprüfen Sie, ob das NLB-VLAN erstellt wurde. Es wird empfohlen, ein dediziertes VLAN für den NLB-Datenverkehr einzurichten.

<#root>

C9300-01#

show vlan id 10

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
10   NLB                               active    Te1/0/1, Te1/0/2, Te1/0/3

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
10   enet  100010     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ----------------------------------------
```

2. CKonfigurieren Sie einen statischen MAC-Adresseintrag für die Ports, die diesen NLB-Datenverkehr empfangen müssen. Dieser Befehl muss alle Trunk-Ports oder Access-Ports im Pfad zum NLB-Cluster im NLB-VLAN enthalten. Im Diagramm gibt es nur einen Pfad zum NLB über Tengig1/0/2.

<#root>

C9300-01(config)#

mac address-table static 0100.5e01.0155 vlan 10 interface TenGigabitEthernet 1/0/2

C9300-01#

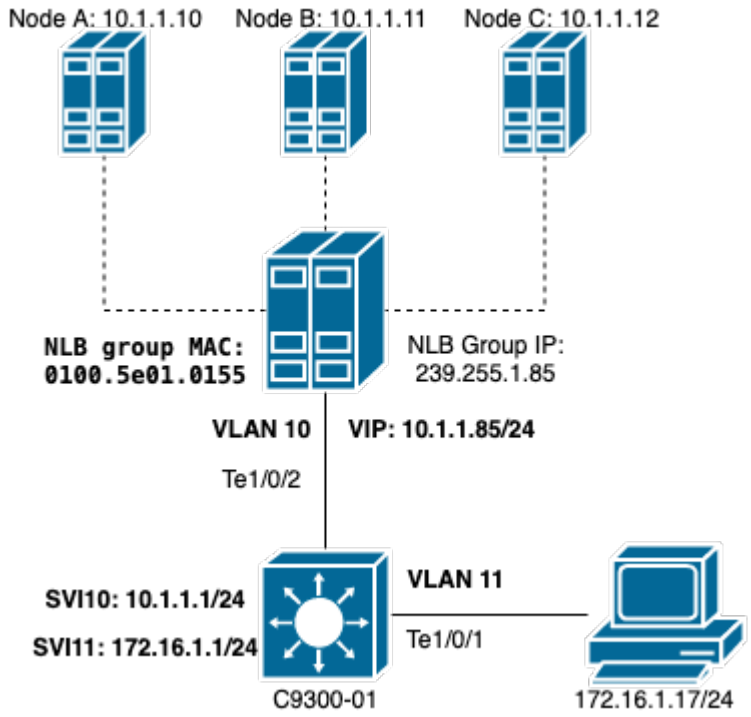
show run | in mac

```
mac address-table static 0100.5e01.0155 vlan 10 interface TenGigabitEthernet1/0/2
```

> **Hinweis**: Der Eintrag der statischen MAC-Adresse kann beliebig viele zugeordnete Ports enthalten. Diese Port-Zuordnung reduziert die erwartete Überlastung innerhalb des VLAN des NLB. In diesem Beispiel kann der statische MAC-Eintrag verhindern, dass der Datenverkehr zum NLB-Cluster aus Te1/0/3 geflutet wird.

Quelle und Ziel in verschiedenen VLANs

Netzwerkdiagramm



In diesem Abschnitt wird beschrieben, wie Sie den NLB konfigurieren, wenn sich der Cluster und die Benutzer in unterschiedlichen VLANs befinden.

1. Konfigurieren Sie das NLB-VLAN und eine IP-Adresse als Standard-Gateway des NLB-Clusters.

<#root>

C9300-01#

show vlan id 10

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
10   NLB                              active    Te1/0/2, Te1/0/3

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
10   enet  100010     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

C9300-01#
```

show run interface vlan 10

```
Building configuration...

Current configuration : 59 bytes
!
interface Vlan10
 ip address 10.1.1.1 255.255.255.0
```

```
end
```

2. Konfigurieren Sie einen statischen ARP-Eintrag für die virtuelle IP-Adresse der NLB-Clusterserver. Der statische ARP muss auf allen Layer-3-Geräten konfiguriert werden, die über eine Switch Virtual Interface (SVI) im Cluster-VLAN verfügen. Der Zweck des statischen ARP besteht darin, dem Switch die Umschreibungsinformationen zu ermöglichen, die zum Senden gerouteter Pakete an das NLB-VLAN erforderlich sind.

<#root>

C9300-01(config)#

arp 10.1.1.85 0100.5e01.0155 arpa

3. Überprüfen Sie das auf dem Access Layer erstellte Benutzer-VLAN und sein Standard-Gateway. Es ist wichtig, dass Sie das Standard-Gateway auf beiden Seiten konfigurieren. (NLB-Cluster und Benutzer).

<#root>

C9300-01#

show vlan id 11

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
11   Users2                           active    Te1/0/1, Te1/0/4

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
11   enet  100011     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

C9300-01#

show run interface vlan 11

```
Building configuration...

Current configuration : 59 bytes
!
interface Vlan11
 ip address 172.16.1.1 255.255.255.0
end
```

Hinweis: Jedes Paket, das nach dem Umschreiben des MAC-Headers geroutet wird, dessen Ziel-MAC-Adresse nicht in der Ausgangs-SVI gelernt wurde, wird dann im entsprechenden VLAN

---

geflutet. Um eine Überlastung zu vermeiden, müssen Sie ein Gateway und ein separates VLAN nur für die NLB-Server erstellen. Wenn Sie kein dediziertes VLAN für den NLB-Datenverkehr konfigurieren möchten, können Sie einen statischen MAC-Adresseintrag für die Ports konfigurieren, die den NLB-Datenverkehr empfangen müssen, d. h. **MAC-Adresstabelle statisch** *0100.5exx.xxxx* **vlan** *#* **interface** *interface_name*

Fehlerbehebung

1. Überprüfen Sie, ob die statischen MAC-Adressen für alle Zielports konfiguriert sind, die den Datenverkehr an den NLB weiterleiten müssen.

<#root>

C9300-01#

show mac address multicast

```
Vlan Mac Address Type Ports
---- ----------- ---- -----
10 0100.5e01.0155 USER Te1/0/2
```

2. Bei Bereitstellungen, bei denen sich der NLB-Cluster in einem anderen Subnetz als die Clients befindet, prüfen Sie, ob statische ARP-Einträge vorhanden sind, die die virtuelle IP des NLB-Servers mit seiner Multicast-MAC-Adresse verknüpfen.

<#root>

C9300-01#

show run | in arp

```
arp 10.1.1.85 0100.5e01.0155 ARPA
```

C9300-01#

show ip arp

```
Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.1.1.1 - c4c6.0309.cf46 ARPA Vlan10
Internet 10.1.1.85 - 0100.5e01.0155 ARPA
Internet 172.16.1.1 - c4c6.0309.cf54 ARPA Vlan11
```

3. Pingen Sie an die IP-Adresse des NLB-Servers mit einer Größe, die nicht häufig verwendet wird. Löschen Sie die Controller des Ports, und überprüfen Sie mit mehreren Iterationen des Befehls, welche Größe nicht so häufig verwendet wird.

<#root>

C9300-01#

show controllers ethernet-controller Te1/0/2 | in 1024

```
0 1024 to 1518 byte frames 0 1024 to 1518 byte frames
```

```
C9300-01#
```

clear controllers ethernet-controller Te1/0/2

```
HOST#
```

ping 10.1.1.85 time 0 rep 1000 size 1024

```
Type escape sequence to abort.
Sending 1000, 1024-byte ICMP Echos to 10.1.1.85, timeout is 0 seconds:
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................
Success rate is 0 percent (0/1000)
```

4. Überprüfen Sie, ob die Pings vom Zielport ordnungsgemäß weitergeleitet wurden und ob derselbe Ping-Test an andere Ports weitergeleitet wurde. Überprüfen Sie dies mit demselben Controller-Zählerbefehl für die verschiedenen Schnittstellen.

<#root>

```
C9300-01#
```

show controllers ethernet-controller Te1/0/1 | in 1024

```
 <-- Ingress Host port
0 1024 to 1518 byte frames 1000 1024 to 1518 byte frames
```

```
C9300-01#
```

show controllers ethernet-controller Te1/0/2 | in 1024

```
 <-- Egress port to NLB
1000 1024 to 1518 byte frames 0 1024 to 1518 byte frames
```

5. Nehmen Sie Paketerfassungen am Eingangs-Port mit EPC und am Ausgangs-Port mit SPAN vor, und überprüfen Sie, ob der Switch die Daten weiterleitet oder nicht.

<#root>

```
C9300-01#
```

monitor capture tac buffer size 10 match any interface Te1/0/1 in

```
C9300-01#
monitor capture tac start
C9300-01#
monitor capture tac stop
C9300-01#
monitor capture tac export location flash:DataTraffic.pcap
```

> **Tipp:** Die Embedded Packet Capture (EPC)-Funktion ist zuverlässig, wenn Pakete in Eingangs- oder Ausgangsrichtung von Layer 2 weitergeleitet werden. Wenn der Datenverkehr jedoch vom Switch geroutet und dann an den Ausgangsport weitergeleitet wird, ist der EPC nicht zuverlässig. Verwenden Sie die SPAN-Funktion (Switch Port Analyzer), um ausgehende Pakete nach dem Layer-3-Routing zu erfassen.

<#root>

C9300-01(config)#

```
monitor session 1 source interface Te1/0/2 tx
C9300-01(config)#
monitor session 1 destination interface Te1/0/3 encapsulation replicate

C9300-01#
show monitor session all
Session 1
---------
Type : Local Session
Source Ports :
TX Only : Te1/0/2
Destination Ports : Te1/0/3
Encapsulation : Replicate
Ingress : Disabled
```

Zugehörige Informationen

- **Catalyst Switches für Microsoft Network Load Balancing - Konfigurationsbeispiel**
- **Technischer Support und Downloads von Cisco**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.